Forensic techniques to investigate emerging trends

Jenna Voss, Masako Asaka and Umair Nadeem
Forensic Risk Alliance

In summary

This article explores cryptocurrencies and ESG in the context of fraud and compliance investigations. FRA considers the pertinent aspects of the evolving regulatory landscape and discusses specific nuances, considerations, and investigative tools practitioners should consider when conducting investigations in these areas, including examples of how they can be applied.

Discussion points

- Regulatory guidance and enforcement trends in cryptocurrencies, with a focus on the US Department of Justice (DOJ), US Securities and Exchange Commission (SEC) and the Financial Crimes Enforcement Network (FinCEN)
- Cryptocurrency investigation considerations and the nuances practitioners should consider when applying standard investigative techniques, as well as how emerging technologies can be leveraged within an investigation
- Regulatory guidance and enforcement trends in ESG-related fraud and compliance investigations by the DOJ, SEC and the US Customs and Border Protection (CBP)
- ESG investigation considerations and the increased reputational risk to companies that are held out to be acting irresponsibly

Referenced in this article

- US Department of Justice, Report of the Attorney General's Cyber Digital Task Force, Cryptocurrency Enforcement Framework, October 2020
- Application of Financial Crimes Enforcement Network's Regulations to Certain Business Models Involving Convertible Virtual Currencies, May 2019
- The Department of Justice's seizure of US$2.3 million in cryptocurrency paid to the ransomware extortionists DarkSide
- Launch of the DOJ's first-ever Office of Environmental Justice within the Environment and Natural Resources Division, May 2022
- SEC's charge of Vale SA for misleading investors about the safety of Brumadinho dam prior to its collapse, April 2022
- SEC's charge of BNY Mellon Investment Adviser, Inc. for misstatements and omissions concerning ESG considerations, May 2022

Introduction

The ever-changing economic, commercial and regulatory landscape, along with emerging technologies, has led to an increase in the sophistication and complexity of fraud schemes.[1] It is essential for investigations practitioners to understand these evolving trends, and how to apply existing and new investigative techniques and technology solutions when issues arise. Within the Americas, the United States continues to set new precedents in regulatory investigations and enforcement actions. The Biden administration has been aggressively pursuing strategies to strengthen 'national security, economic equity, global anti-poverty and development efforts, and democracy itself,'[2] announcing new government-wide efforts aimed at curbing white-collar crime. Foreign Corrupt Practices Act (FCPA) enforcement continues to be a critical priority for the US Department of Justice (DOJ) and the US Securities & Exchange Commission (SEC), with high-profile enforcement actions including *Stericycle* and *Glencore* dominating recent headlines. In addition to historical priority areas, regulatory agencies across the Americas – including the DOJ and SEC – have indicated that they will now be focusing investigative efforts and resources on misconduct in the emerging areas of cryptocurrencies and environmental, social and governance (ESG), and sanctions violations related to Russia's war on Ukraine.

In this article, we explore cryptocurriencies and ESG in the context of fraud and compliance investigations. While not intended to be a fulsome discussion of current regulations, we briefly touch upon pertinent aspects of the evolving regulatory framework in the Americas that investigators should be aware of. We then discuss specific nuances, considerations, and investigative tools that practitioners should consider when conducting investigations in these areas, including examples of how they have been applied in recent investigations.

Cryptocurrencies

Cryptocurrencies have been around for over a decade, yet have only recently been accepted as more mainstream forms of investment and finance. These digital assets allow for faster fund transfers across the globe and provide increased transaction transparency. Their decentralised nature also allows them to exist outside the control of governments and central banks.[3] The exponential growth in the use of cryptocurrencies has even led several countries to formally accept them as legitimate forms of payment. In October 2021, El Salvador became the first of many countries to adopt the cryptocurrency, Bitcoin, as

1 https://www.law.com/nationallawjournal/2022/06/29/the-intelligence-factor-a-valuable-resource-in-investigations/.
2 https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/06/fact-sheet-u-s-strategy-on-countering-corruption/.
3 https://www.investopedia.com/terms/c/cryptocurrency.asp.

legal tender.[4] However, price volatilities and nascent regulatory oversight have allowed some bad actors to take advantage of the investing public by leveraging cryptocurrencies as conduits for fraudulent activities. We are now seeing a wide range of schemes perpetrated through the use of cryptocurrencies, including traditional frauds such as bribery, embezzlement, money laundering, pump and dump schemes, and Ponzi schemes. According to a February 2022 report, funds sent to illicit addresses reached US$14 billion in 2021, doubling from US$7.8 billion in 2020 – which is extremely high given cryptocurrency's market value of approximately US$1.8 trillion, as of the date of the report.[5]

Regulatory guidance and enforcement trends in cryptocurrencies

Due to the decentralised nature and complexity of cryptocurrencies, regulators have been slow to provide guidance and enact specific frameworks for regulation. Until recently, cryptocurrencies were essentially operating in the 'wild west' with limited to no oversight and sporadic regulatory enforcement. Recent incidents, however, like the collapse of the Terra Luna cryptocurrency, which wiped away roughly US$60 billion in value, highlight the desperate need for regulatory oversight around the creation, marketing and trade of cryptocurrencies. In a speech to the Senate on 12 May 2022, the United States Treasury Secretary, Janet Yellen, acknowledged the risks of cryptocurrencies to the US economy and stated that she 'wouldn't characterize it at this scale as a real threat to financial stability, but they're growing very rapidly and they present the same kind of risks that we have known for centuries in connection with bank runs.'[6]

Given this changing landscape, several US regulatory agencies are now actively focused on cryptocurrencies, and the DOJ, the SEC and the Financial Crimes Enforcement Network (FinCEN) appear to be taking the global lead on investigations and enforcement. We highlight below key elements of applicable guidance from these regulators most pertinent for investigative professionals to consider in fraud and compliance investigations.

DOJ

In October 2020, the DOJ released the Cryptocurrency Enforcement Framework[7] that discusses how cryptocurrency technology is currently used and how malicious actors have misused the technology. The framework outlines the three primary ways that criminals commit fraud using cryptocurrencies:

4 https://www.npr.org/2021/09/07/1034838909/bitcoin-el-salvador-legal-tender-official-currency-cryptocurrency.
5 Chainalysis 2022 Crypto Crime Report. https://go.chainalysis.com/2022-Crypto-Crime-Report.html.
6 https://www.bloomberg.com/news/videos/2022-05-12/yellen-says-threats-of-crypto-are-growing-video.
7 https://www.justice.gov/archives/ag/page/file/1326061/download.

1. using cryptocurrency to commit crimes or support terrorism;[8]
2. using cryptocurrency to hide financial activity;[9] and
3. committing crimes within the cryptocurrency marketplace itself.[10]

The framework goes on to identify the key legal authorities and partnerships the DOJ relies upon to combat these threats and discusses the Department's approaches for addressing the growing challenges presented by cryptocurrencies. Additionally, the framework provides insights on the intricacies of cryptocurrency transactions and highlights tools, such as blockchain analysis, which can assist in identifying illicit transactions to real-world identities by tracing the transaction path of various cryptocurrency transactions.[11]

The Fraud Section of the DOJ is actively utilising this framework to investigate cryptocurrency-related matters, specifically referencing it in its press release related to the February 2022 seizure of US$3.6 billion in cryptocurriences related to the indictment of a New York couple on charges of conspiring to launder cryptocurrency valued at US$4.5 billion, which had been stolen in a 2016 hack of the cryptocurrency exchange Bitfinex.[12]

SEC

In 2017, the SEC created the Crypto Assets and Cyber Unit tasked with 'policing wrongdoings in the crypto markets while continuing to identify disclosure and controls issues with respect to cybersecurity.'[13] The SEC continues to add headcount to the unit and although they have not yet published any cryptocurrency-specific guidance, they did file 20 cryptocurrency-related

8 Such as using cryptocurrencies to buy or sell illegal items, committing extortion via ransomware or blackmail, or using cryptocurrency technology to raise funds for criminal or terrorist activity – DOJ Cryptocurrency Enforcement Framework, pp. 5–16.

9 Such as using cryptocurrencies to launder money obtained through illegitimate means, conducting transactions in cryptocurrency to avoid sanctions, or facilitating illegal transactions on cryptocurrency exchanges that do not have stringent AML or KYC requirements – DOJ Cryptocurrency Enforcement Framework, pp. 5–16.

10 Such as using cryptocurrency to launder money obtained through illegitimate means, conducting transactions in cryptocurrency to avoid sanctions, or facilitating illegal transactions on cryptocurrency exchanges that do not have stringent AML or KYC requirements – DOJ Cryptocurrency Enforcement Framework, pp. 5–16.

11 Cryptocurrency Enforcement Framework, p. 14.

12 According to the DOJ press release, the couple utilised a series of sophisticated techniques to illegally obtain control of approximately 120,000 bitcoins in 2016. They then proceeded to withdraw millions of dollars through Bitcoin ATMs and make large purchases of non-fungible tokens (NFTs), gold and gift cards. Following the arrest, the department seized US$3.6 billion in cryptocurrency, marking it as the 'largest ever' financial seizure by the DOJ. https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency.

13 https://www.sec.gov/news/press-release/2022-78.

enforcement actions in 2021 – a significant increase from the five to 10 annual enforcement actions in prior years.[14]

Notably, in March 2022, the SEC charged siblings John and JonAtina Barksdale – dubbed the 'snake-oil salesmen' – with defrauding approximately 20,000 investors out of more than US$124 million through two unregistered fraudulent offerings called Ormeus Coin.[15]

FinCEN

In May 2019, FinCEN issued guidance consolidating current FinCEN regulations and related administrative rulings and guidance. The agency also refreshed the scope of these pronouncements to explicitly include cryptocurrencies, and clarified when businesses involving cryptocurrencies will be subject to the Bank Secrecy Act (BSA).[16]

According to FinCEN, users who obtain cryptocurrency in order to purchase goods or services are not generally considered money transmitters subject to FinCEN's authority. However, issuers, redeemers, and exchangers of cryptocurrency do fall within the realm of FinCEN's regulatory authority, requiring them to adhere to applicable AML and KYC statutes. Utilising this updated guidance, in August 2021, FinCEN assessed a civil penalty in the amount of US$100 million[17] against BitMEX, one of the oldest and largest cryptocurrency derivatives exchanges, for blatant violations of the BSA.

Prior to this, in October 2020, FinCEN also assessed a US$60 million civil penalty against Larry Dean Harmon, the founder of Helix and Coin Ninja, for violations of the BSA and operating unregistered money services businesses.[18] His companies Helix and Coin Ninja were operating as cryptocurrency 'mixers' or

14 https://www.cornerstone.com/wp-content/uploads/2022/01/SEC-Cryptocurrency-Enforcement-2021-Update.pdf.

15 From June 2017 to March 2022, the siblings offered and sold Ormeus Coin to investors on cryptocurrency trading platforms and promoted their offering through roadshows worldwide, YouTube videos, press releases, social media posts, and other media outlets. Both siblings falsely claimed that the Ormeus Coin had US$250 million in crypto mining operations, producing between US$5.4 and US$8 million in revenue per month. In reality, they had abandoned their crypto mining operations and were utilising investor funds for their own personal gain, such as lavish purchases and trips around the globe. https://www.sec.gov/news/press-release/2022-37.

16 'Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (CVC)', https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-certain-business-models.

17 https://www.fincen.gov/news/news-releases/fincen-announces-100-million-enforcement-action-against-unregistered-futures.

18 It is important for the investigators to understand applicable regulations – including across relevant jurisdictions – in order to understand relevant compliance requirements and the expectations of the various regulators who may have jurisdiction in the matter. https://www.fincen.gov/news/news-releases/first-bitcoin-mixer-penalized-fincen-violating-anti-money-laundering-laws.

'tumblers', which are special cryptographic services that can be used for money laundering as they help anonymise blockchain transactions and addresses.

Cryptocurrency investigation considerations

While regulators continue to develop cryptocurrency-specific regulations, the enforcement actions thus far make a clear statement that existing regulation such as those related to anti-money laundering, do apply. In the same light, many investigative techniques used to investigate matters involving cryptocurrencies – such as the use of transactional testing to substantiate bribery allegations – should already be familiar to practitioners.

In this section we explore the nuances that practitioners should consider when applying standard investigative techniques, as well as how emerging technologies can be leveraged within the investigation.

Planning for the investigation

In commencing an investigation related to cryptocurrencies, there are several considerations that investigative teams should evaluate carefully during the planning and scoping phases. Conflicting global trends and differing regulatory guidance, coupled with increasingly severe criminal penalties and civil fines for violations, require investigative teams to take into account the varying levels of regulations, across jurisdictions, that may be applicable. In instances where specific cryptocurrency regulations do apply, practitioners should use them as a guide for conducting the investigation. For example, if a practitioner is investigating suspicious transactions that have occurred within a Virtual Asset Service Provider (VASP) as defined within US regulations, the practitioner should consult the BSA as the updated guidance indicates that VASPs are considered money transmitters and therefore subject to compliance with AML requirements under the BSA. If the VASP had inadequate controls to monitor and report suspicious activity, then it is likely that fraudulent transactions could be perpetrated due to the lack of these controls.

Taking the time to consider the nuances and complexities that may arise within the investigation will also help the investigation team determine any required involvement of subject matter experts. Such investigations should be staffed with experts who are well versed in the elements that make up a cryptocurrency transaction, including cryptocurrency addresses, wallets, exchanges and the blockchain. They should also have a thorough understanding of how these elements come together to 'tell the story' of what occurred. In addition to understanding cryptocurrencies, investigation teams should include

professionals familiar with available blockchain analytic tools, which are discussed in more detail in the following sections.

Identifying information relevant to the investigation

For cryptocurrency-related investigations, data collection and analysis will be a major component of the overall investigative procedures. Core data points that require review will include the applicable cryptocurrency blockchains. Blockchains are public ledgers for cryptocurrencies that are accessible by virtually anyone, and in terms of investigations, these blockchains serve as audit trails which practitioners leverage to trace transactions of interest.

Although one can trace specific transactions within the blockchain, further data collection is typically required to identify the details of real-world actors associated with pseudonymous cryptocurrency addresses identified on the blockchain. Therefore, additional points of data requiring review and analysis include emails, text messages and other structured or unstructured data stored on devices that could potentially identify the owners of cryptocurrency addresses, as well as information on wallet private keys or passwords associated with the addresses. Forensic data experts are typically well versed in procedures and tools necessary for accurately collecting and preserving data while offering extensive multi-jurisdictional data privacy, transfer and protection expertise.

Investigative procedures

Cryptocurrency investigations often involve tracing assets in order to identify where funds went and what parties were involved. Instead of traditionally tracing funds through the general ledger and corresponding bank statements where the crime was committed using fiat currency, practitioners will be investigating cryptocurrency activity recorded on the blockchain.

Complications sometimes arise when multiple cryptocurrencies are being used to facilitate the illicit activity. Not all cryptocurrencies are maintained on a single blockchain, therefore tracing across different blockchains will likely be required if multiple cryptocurrencies were used at any point in the payment process. This is where blockchain analytic tools can provide value to the investigation. Blockchain analytic tools streamline the review as they collate copious amounts of blockchain data, across multiple blockchains, and provide innovative data visualisations that allow for methodical asset tracing and effective reporting of findings. By utilising blockchain analytic tools in tandem with the information collected in the data collection phase to identify owners of cryptocurrency addresses, practitioners will be able to capture and analyse cross-chain cryptocurrency transactions in a more tactical manner, increasing the speed with which the investigation can be conducted.

The FBI's seizure of US$2.3 million in bitcoins from DarkSide – a group of cybercriminals who extorted large sums of cryptocurrency from various organisations through ransomware attacks – demonstrates how data collection and blockchain analytic tools can be crucial in an investigation involving cryptocurrency.[19] In May 2021, DarkSide attacked Colonial Pipeline, resulting in the temporary disablement of Colonial Pipeline's operations. Colonial Pipeline alerted the FBI of the attack, and the DOJ's newly formed Ransomware and Digital Extortion Task Force acted quickly in 'following the money' utilising a blockchain analytics tool. This allowed the FBI to automate the process of tracing and visualising the flow of funds from voluminous blockchain data sets. Further, the analytics tool allowed for the FBI to determine that the scheme was perpetrated through transferring funds among multiple addresses. The ultimate transfer of Colonial Pipeline's payment was to a DarkSide affiliate address that had been identified as previously receiving bitcoin payments from a separate ransomware called NetWalker, which the FBI had previously investigated and seized ill-gotten cryptocurrency. With the FBI's knowledge of the private key associated with the DarkSide address and thorough tracking of the various transactions that took place, the FBI was able to successfully seize nearly 63.7 bitcoins valued at US$2.3 million.

Environmental, social and governance (ESG)

ESG has increasingly been a topic of focus as investors, consumers, employees and activists place pressure on companies and individuals to meet growing expectations to demonstrate good corporate citizenship. Regulators worldwide have responded, placing more scrutiny and higher expectations of transparency on how companies govern these topics. In turn, this intensified pressure has created motives for companies to subvert regulations and investor expectations by committing fraudulent acts, delivering false, inaccurate or manipulating and misleading disclosures in (eg, 'greenwashing' information related to emissions, supply chain or activities-related sustainability), ESG-related data.

While this holistic focus on ESG represents an emerging trend, many of the key elements underpinning this movement have been considered by companies – in various forms and to different degrees – for many decades. For example, major companies around the world have issued corporate social responsibility (CSR) reports as a best practice for years, with these reports communicating the 'E' and 'S' components of ESG.[20] Such reporting has been particularly relevant for

19 https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside#:~:text=June%207%2C%202021-,Department%20of%20Justice%20Seizes%20%242.3%20Million%20in%20Cryptocurrency%20Paid%20to,valued%20at%20approximately%20%242.3%20million.

20 According to Governance & Accountability Institute, 90 per cent of S&P 500 Index Companies published sustainability reports in 2019: https://www.ga-institute.com/storage/press-releases/article/90-of-sp-500-index-companies-publish-sustainability-reports-in-2019-ga-announces-in-its-latest-a.html.

companies operating mines, refineries, and oil and gas fields subject to local environmental regulations and contractual obligations to restore the environment (eg, water quality). Similarly, the potential use of 'conflict minerals' – mined resources used to influence and finance armed conflict, human rights abuses, and violence[21] – would now be considered a relevant supply-chain issue under the 'S' of ESG. Yet companies in the minerals and gemstones industry have been familiar with such issues for over 10 years, with the formal adoption in 2012 of the SEC's conflict minerals rule[22] pursuant to the Dodd-Frank Act of 2010.

Regulatory guidance and enforcement trends in ESG

With the global prevalence of many of the relevant ESG issues and the breadth of the scope across an entity's operations (eg, from engineering and manufacturing to finance and marketing), multiple regulators have jurisdiction over various aspects of ESG. US regulators currently appear to be more active at this stage than other regulators in the Americas in positioning to oversee ESG topics.

Still, certain key US regulators, including the DOJ and SEC, are in the nascent stages of issuing meaningful ESG guidance. Others, including the US Customs and Border Protection (CBP), have already been active in governing the sourcing and importing practices of companies operating in the US. We highlight below key elements of the current (and expected) guidance from these regulators most pertinent for investigative professionals to consider in fraud and compliance investigations.

DOJ

In May 2022, the DOJ announced a series of actions to advance environmental justice and strengthen the DOJ's commitment to ensuring equal justice, including a launch of its first-ever Office of Environmental Justice within the Environment and Natural Resources Division, signalling further possible enforcement actions by the DOJ.[23,24]

21 https://earthworks.org/issues/conflict-minerals/.

22 Section 1502 of the Dodd-Frank Wall Street Reform and Consumer Protection Act requires 'issuers with conflict minerals that are necessary to the functionality or production of a product manufactured by such person to disclose annually whether any of those minerals originated in the Democratic Republic of the Congo or an adjoining country.' If an issuer's conflict minerals originated in those countries, the issuer is required 'to submit a report to the Commission that includes a description of the measures it took to exercise due diligence on the conflict minerals' source and chain of custody.' https://www.sec.gov/rules/final/2012/34-67716.pdf.

23 https://www.justice.gov/opa/pr/justice-department-launches-comprehensive-environmental-justice-strategy.

24 https://www.justice.gov/ag/page/file/1499236/download.

The DOJ has issued limited enforcement actions to date, but notably announced in March 2022 a settlement of approximately US$121 million[25] with Chevron Phillips Chemical Company LP.[26] The DOJ determined the company violated the Clean Air Act through three facilities in Texas which emitted excessive amounts of toxic pollution via industrial flares.

SEC

The SEC's mission is to protect investors, which has led to the SEC prioritising ESG within its agenda given heightened investor interest in this topic.[27] In March 2021, the SEC announced its formation of a Climate and ESG Task Force in the Division of Enforcement, mandated with identifying material gaps or misstatements in issuers' climate risk disclosures in annual financial reporting under existing rules. A year later, in March 2022, the SEC followed with its proposed climate-related disclosure requirements rule designed to improve and bring consistency to the climate-related disclosures of public companies. If the SEC's proposal is approved, public companies will need to act quickly to implement measures to meet Greenhouse Gas (GHG) emissions disclosure requirements by fiscal year ending 2023 or 2024.[28]

The SEC has been active in issuing enforcement actions, and we highlight here two recent matters. First, in April 2022, the SEC raised complaints against Vale, SA (Vale), a publicly traded Brazilian mining company, for making false and misleading claims about the safety of its dams prior to the deadly collapse of the Brumadinho dam in the Brazilian state of Minas Gerais in January 2019. According to the SEC, this disaster led to a loss of more than US$4 billion in Vale's market capitalisation and Vale was allegedly in violation of anti-fraud and reporting provisions of the federal securities laws for manipulating dam safety audits and obtaining numerous fraudulent stability declarations to mislead governments, communities, and investors.[29, 30]

25 Comprising a civil penalty of US$3.4 million civil penalty along with a requirement to spend an estimated US$118 million on compliance improvements.
26 https://www.justice.gov/opa/pr/chevron-phillips-chemical-company-agrees-reduce-harmful-air-pollution-three-us-chemical.
27 https://www.sec.gov/about/reports/sec-fy2014-agency-mission-information.pdf.
28 The proposed disclosure requirements employ a phased-in approach depending on the registrant types to accommodate the newly proposed regulations: the current proposed timeline will require the filers to provide greenhouse gas (GHG) emission disclosures as of the fiscal year ending 2023 for large accelerated filers (for Scope 1 and Scope 2). Large accelerated filers will also need to disclose Scope 3 GHG emissions as of the fiscal year ending 2024 and in the same year, attestation on Scope 1 and Scope 2 GHG emission disclosure will require limited assurance; they will have two more years to obtain reasonable assurance (ie, 2026). Accelerated and non-accelerated filers will have an additional year whereby they will need to provide GHG emissions for Scope 1 and Scope 2 by fiscal year ending 2024, and Scope 3 disclosure by fiscal year ending 2025. https://www.sec.gov/rules/proposed/2022/33-11042.pdf.
29 https://www.sec.gov/news/press-release/2022-72.
30 https://www.sec.gov/litigation/complaints/2022/comp-pr2022-72.pdf.

Second, in May 2022, the SEC charged BNY Mellon Investment Adviser, Inc. (BNY Mellon) with making material misstatements and omissions concerning how it had evaluated ESG considerations in its investment decisions. BNY Mellon claimed that from July 2018 to September 2021, all investments in certain mutual funds had undergone an ESG quality review. However, the SEC found that numerous investments held in these funds lacked an ESG quality review score at the time of investment. Further, BNY Mellon did not have policies and procedures that were adequately designed to prevent inaccurate or materially incomplete statements in its representations.[31] BNY Mellon agreed to pay a US$1.5 million penalty to settle the charges.

CBP

The CBP is responsible for establishing and enforcing regulations enacted to safeguard the US's borders and points of entry.[32] Many of its regulations have relevance to ESG, including the Smoot-Hawley Tariff Act, which has banned the US import of any goods made with forced labour since 1930.

More recently, issues around Uyghur minorities including concerns of forced labour in Xinjiang, internment camps and genocide have garnered attention from the US and the rest of the world. Relatedly, on 23 December, 2021, the Uyghur Forced Labor Prevention Act (UFLPA) was signed into US federal law, introducing additional rules around imports into the US as part of a policy to ensure that goods made with forced labour in the Xinjiang Uyghur Autonomous Region (XUAR, or Xinjiang) of the People's Republic of China (China) do not enter the US market. The UFLPA, which the CBP is responsible for enforcing, stipulates that unless importers can present clear and convincing evidence that goods, wares, articles and merchandise mined, produced or manufactured in China's XUAR are free from forced labour, it is prohibited for entities to import these products into the US.[33] The CBP published 'Uyghur Forced Labor Prevention Act: US Customs and Border Protection Operational Guidance for Importers' (CBP Operational Guidance) on 13 June 2022[34] and this rebuttable presumption went in to effect on 21 June 2022.[35] This law impacts the second-largest cotton producer in the world, and any parties that have a business relationship with

31 https://www.sec.gov/news/press-release/2022-86.
32 https://www.cbp.gov/about.
33 Uyghur Forced Labor Prevention Act. https://www.cbp.gov/trade/forced-labor/UFLPA?language_content_entity=en.
34 Uyghur Forced Labor Prevention Act: US Customs and Boarder Protection Operational Guidance for Importers, dated 13 June 2022. https://www.cbp.gov/sites/default/files/assets/documents/2022-Jun/CBP_Guidance_for_Importers_for_UFLPA_13_June_2022.pdf.
35 This is particularly a significant development for business entities that are importing high-risk commodities from China, such as cotton, polysilicon, and tomatoes because according to recently published CBP Operational Guidance they are 'presumed to be made with forced labor are prohibited from entry' in to the US and this presumption applies to goods that are 'made in, or shipped through [China] and other countries that include inputs made in Xinjiang.'

China, sending a clear message that US regulators and enforcement agencies are taking a strict stance against the use of forced labour.

In June 2022, the CBP issued its 'Green Trade Strategy', which 'establishes a proactive model to combat the negative impacts of climate change on the agency's trade mission while strengthening existing enforcement activities against environmental trade crimes including illegal logging; wildlife trafficking; illegal, unreported, and unregulated fishing; and illegal mining.'[36]

ESG investigation considerations

Despite the seemingly slow-paced development of ESG regulations – which may be appreciated in some forums given the additional compliance, monitoring and reporting burden they will place on companies – enforcement in this area is clearly on the rise. Practitioners investigating potential ESG related violations will need to be acutely aware of the increased reputational risk to companies that are held out to be acting irresponsibly with respect to people and the planet. We see the stakeholders of an investigation broadening as investigative journalists and environmentalists place companies under intense scrutiny and alert investors and the general public to potential ESG related wrongdoing. While practitioners will still rely on many standard investigation techniques, they should expect to supplement those with more nuanced approaches that will aid in navigating the new territory and complexities that they may encounter in ESG investigations, as we explore in this section.

Planning for the investigation

In commencing an investigation related to ESG matters, there are several considerations practitioners should evaluate carefully during the planning and scoping phases. It is important for the investigators to evaluate applicable regulations – including across relevant jurisdictions – in order to understand relevant compliance requirements and the expectations of the various regulators who may have jurisdiction in the matter. This evaluation will also help practitioners determine whether the investigative team should be supplemented with subject matter experts. Such individuals can be instrumental in supporting the investigation by, for example, designing nuanced testing procedures for the investigation, interpreting complex regulatory requirements in different jurisdictions, and evaluating highly technical manuals and procedures.

In 2015, the DOJ, Environmental Protection Agency (EPA) and CBP charged Volkswagen AG for participating in a conspiracy to defraud the United States and VW's US customers and to violate the US Clean Air Act by lying and misleading the

36 https://www.cbp.gov/trade/cbp-green-trade-strategy.

EPA and US customers by manipulating the emission levels of nitrogen oxides of diesel vehicles during regulatory testing to meet emissions standards.[37] Outside of this test mode, the software allowed the engine to substantially exceed legal emissions limits. Referred to as 'Dieselgate', Volkswagen AG was required to pay a penalty of US$4.3 billion and an independent compliance monitor was mandated for a period of three years. Multiple other companies have since been implicated in the Dieselgate scandal. In such an investigation, practitioners may consider including in its team regulatory experts specialising in the Clean Air Act, automotive engineers with a background in vehicle programming, and automotive safety experts with knowledge of regulatory emission testing processes and requirements.

Identifying information relevant to an investigation

There are several considerations for practitioners around identifying and obtaining data and information relevant to an ESG investigation, since the nature of the allegations may necessitate reviewing information beyond the traditional data sources relevant to many types of investigations (eg, financial records and general ledger data). The nature of the allegations will guide identification of information relevant to the investigation, and practitioners will need to dedicate time to understand what type of information may be useful or necessary to review.

An investigative team should be prepared to encounter challenges related to data, as it is highly possible to encounter an even broader range of data sets and systems than is relevant in other types of investigations. Many of these systems may be 'home-grown' by companies and developed to adapt to new needs for data in areas beyond those that have traditionally been tracked, analysed, reported on and audited. ESG investigations that require analysis of supply chains may also present challenges, as certain data points may not be tracked by the company, and may not even be accessible without involving third parties. Data analytics experts, with the ability to understand the back-end database design of non-standard systems, will be essential in assessing what data exists and extracting the relevant data to prepare for the investigative analysis.

In the Dieselgate case, data sets of testing results from multiple vehicle models, along with data gathered from vehicles while in operation, would be critical to this type of information. If automotive manufacturers performed this type of testing internally, these data sets would likely reside in a system within their emission testing/inspection facility. Depending on how the data is maintained, it may require scrubbing, formatting and organising to a standard and optimised format before practitioners could use it for analysis. It would also be important

37 https://www.justice.gov/opa/pr/volkswagen-ag-agrees-plead-guilty-and-pay-43-billion-criminal-and-civil-penalties-six.

to obtain the source code from the software, along with any audit logs and approval records for changes to the code.

We have included below two additional examples of the types of data relevant to certain ESG allegations, along with the related challenges that the investigative team may need to address:

- Allegations of human rights and labour practices abuses, or around the use of unsustainably sourced ingredients: the scope of these types of investigations will likely require delving into a company's complex global supply chain. Investigations practitioners should expect to encounter limitations in the data they can reasonably gain access to given the likelihood that multiple third parties, whose data the company has no control over, form part of this chain. To supplement information requests made to in-scope third parties, targeted analysis of unstructured datasets may turn up documents (eg, emails, attachments to emails such as invoices or shipping documents, and meeting invites), or even structured data extracts (supplier transaction extracts, raw material pricing data, etc) that can be used to plug gaps where information is not forthcoming from third parties.
- Allegations of greenwashing related to investments: relevant sources of information will include information about the fund's ESG rating or scorecard, the basis upon which the determination of its ESG rating was made, and the conditions that had to be met to achieve classification as an ESG fund. Further, fund prospectuses should be identified to consider whether statements made have been misstated or could potentially mislead investors.

Investigative procedures

ESG investigations necessarily require a variety of investigative techniques and procedures, given the breadth of topical areas falling within its scope. Investigation teams will need to take a creative approach to crafting testing analysis procedures, including considering how available data can be leveraged, particularly in those areas that have not typically been monitored and tested historically. Variable factors such as size of the data, scope of the matter and the severity of an issue can influence the analysis and sampling techniques employed. As referenced earlier in the chapter, it may be helpful to seek assistance from skilled data analytics specialists in collecting and organising data for practitioners to review.

In the 2022 Vale matter, where the SEC charged the Brazilian mining company with misleading investors about the safety of the Brumadihno dam, the SEC's investigation would have required tracing claims made to investors back to source documentation and data to assess the validity of the claims. Among

the allegations, the SEC claimed that Vale knowingly based declarations of stability on unreliable laboratory data and concealed material information from dam safety auditors. Investigative procedures to arrive at these allegations could include: analysing historical laboratory data to assess consistency of test results over time, comparing observations in external safety audits with results of internal audits or other testing, analysing the underlying workpapers from internal reviews and audits, reviewing email correspondence internally and with auditors or third party inspectors, and interviewing relevant employees.

The following examples of allegation-specific procedures illustrate additional types of techniques that practitioners could employ in an ESG investigation:

- Allegations of discrimination and police brutality: analysing metrics around the number of traffic stops involving persons of colour, and the outcome of those stops, compared to the overall statistics for the police department's traffic stops.
- Allegations of greenwashing related to investments: tracing statements made in marketing and investment materials back to working papers, analysis and raw data to assess whether environmental impact disclosures made to potential investors are appropriate and reasonable based on source information.
- Allegations of falsified emissions reporting: utilising software engineers and developers to analyse audit logs of software programming changes and to ascertain whether there are corresponding approved change orders.
- Supply chain investigation: leveraging due diligence records along with sophisticated supply chain traceability technologies to scientifically identify the source of materials included in a finished good, to assess whether the raw materials originated from a region where human rights violations such as child or slave labour are known to be commonplace.

Conclusion

As cryptocurrencies and ESG continue to be top of mind for investors and regulators alike, there will be increasing opportunities and incentives for bad actors to use these focus areas as mechanisms for fraudulent activity and deception. Practitioners should remain aware of the trends and regulatory developments in these areas identified as priorities by multiple regulators in the Americas, and be proactive in developing the necessary tools and techniques required to conduct investigations. As we have described in this article, many of the necessary investigative techniques will be familiar to experienced practitioners, although often requiring a slight nuance to adapt to the nature of the allegations subject to investigation.

* *The authors would like to acknowledge Emma Hodges (partner), Aeriel Davis (manager), Jose Arcos (manager) and Dominique Vidjanagni (senior associate) for their contributions to this article.*

Jenna Voss

Forensic Risk Alliance

Jenna Voss is a partner at FRA with extensive experience in conducting forensic consulting, investigative, and monitorship assignments across multiple industries. She leads teams in performing multi-jurisdictional investigations, advising on anti-corruption and anti-money laundering matters, providing accounting expertise on litigation matters, and devising innovative solutions to guide clients through difficult situations. Jenna has led high-profile forensic assignments globally, and has significant experience in the Americas, including in the United States, Mexico, Ecuador, Brazil and Canada.

Jenna recently led a team in performing a multi-year assessment of a European engineering company as part of a DOJ Monitorship into environmental fraud concerns. She also recently led a global team in performing a multi-year forensic assessment at the direction of the monitor of a Brazilian-based company that engaged in misconduct related to bribery and corruption and oversaw a complex investigative review of inventory and intercompany transactions for a manufacturing company.

Previously, Jenna supported the Mexico operations of a biomedical devices client in enhancing its anti-corruption compliance programme while under a multi-year monitorship. Jenna also has experience conducting whistleblower investigations, leading anti-money laundering assessments, performing accounting and anti-corruption due diligence, building complex financial models and advising financially troubled companies in bankruptcy and restructuring situations.

She is a certified public accountant, certified fraud examiner, certified anti-money laundering specialist and certified in financial forensics and holds master's degrees in business administration and accounting.

Masako Asaka
Forensic Risk Alliance

Masako Asaka has over 18 years of forensic accounting and auditing experience, specialising in fraud investigations and regulatory compliance work. Her expertise includes Foreign Corrupt Practices Act/anti-bribery and corruption, securities fraud, fraud risk management, third party/pre-acquisition due diligence, anti-money laundering and foreclosure review for clients in a variety of industries. Masako works with external and in-house counsel, as well as management of companies to address their concerns and has broad experience dealing with US regulators in her career.

Masako was a lead director of a monitorship of an automotive engineering company in which FRA's founding partner was a DOJ-appointed independent compliance monitor. The monitorship mandate included an evaluation of the company's implementation and enforcement of its corporate compliance, technical compliance and ethics programme.

Her other previous experience includes:

- Serving as a lead director of an aviation supply company monitorship in which FRA was retained to provide forensic accounting support to a DOJ-appointed monitor throughout all phases of the monitorship, delivering particular expertise in respect of the company's internal controls and compliance environment. Over the course of the monitorship, FRA worked with the company's compliance functions, performing FCPA compliance testing and reviews across Asia, Africa, Europe, the Middle East and US.
- Providing accounting support to independent co-monitors related to an enforcement action by the Public Company Accounting Oversight Board (PCAOB) for a member firm of a global network accounting firm which involved reviewing and assessing the audit firm's design and execution of its system of quality control, evaluating tone at the top, ethics helpline system, training programmes and preparing detailed reports related to observations, findings and recommendations .

Prior to joining FRA, Masako was a director of KPMG LLP's Forensic Service, where she was involved in various fraud and FCPA investigations. Before she became a forensic accountant, Masako was as an auditor at KPMG LLP, providing financial statement audit services to clients for over four years, and gaining experience in financial statement audits, SOX and internal control testing. During a short-term assignment in Japan, she assisted JSOX and SOX implementation of Japanese companies.

Masako is a certified public accountant, certified fraud examiner, and holds a Certified in Financial Forensics designation from the American Institute of Certified Public Accountants. She also holds a Bachelor of Science degree in accounting and a Bachelor of Arts degree in international relations.

Umair Nadeem

Forensic Risk Alliance

Umair Nadeem is a director based in FRA's Dallas office and has over 15 years of forensic accounting experience. He specialises in providing consulting and investigative services to private equity firms, external and in-house counsel, audit committees, company management and government entities regarding issues of compliance and regulation, fraud and misconduct, regulatory enforcement actions, and the assessment of financial and legal risks relative to fraud and poor internal controls.

Umair has extensive experience in assisting global organisations to develop and enhance corporate compliance programmes, conducting small and large-scale investigations, as well as leading corporate monitorships, involving allegations of bribery and corruption, potential violations of the US Foreign Corrupt Practices Act, financial statement fraud, embezzlement, asset misappropriation and waste/abuse. Umair also has an established track record of managing large-scale teams, including cross-border teams, to assist clients in effectively resolving their investigative and compliance matters.

Umair recently led teams providing forensic accounting support on criminal defence matters involving allegations of sanctions violations perpetrated by an executive of a global company based in the Middle East as well as a US-based real estate investment trust alleged to be operating as a Ponzi scheme. Currently, Umair is providing forensic accounting support on a DOJ/SEC compliance monitorship of a global financial institution.

Prior to joining FRA, Umair was a director in KPMG's forensic practice where he led the firm's forensic in the audit service line for the southwest region. While at KPMG, Umair worked on some of the firms highest-profile matters including leading a nationwide team of forensic professionals to provide investigative support to BP in relation to the Deepwater Horizon oil spill.

Umair holds a Bachelor of Business Administration in finance from the University of Texas – McCombs School of Business. He is a certified fraud examiner, and a member of the Association of Certified Fraud Examiners and the Society of Corporate Compliance and Ethics.

Forensic Risk Alliance (FRA) is an international consultancy specialising in corruption and fraud investigations, compliance and risk mitigation for major global corporations and law firms. We combine deep forensic accounting and investigative expertise with cutting edge data mining technology to position clients for success as they navigate investigations, litigation and compliance challenges. With 10 locations and datacenters across the Europe and North America, we have extensive cross-sector and cross-border experience and scalability anywhere in the world, harnessing the right mix of collaborative expertise for clients across both developed economies and emerging markets.

We are independent experts and forward-thinking advisers. For more than two decades, we have been trusted by corporates, their counsel, and regulators alike to quickly surface the facts so that controversies can be resolved fairly, efficiently, and without undue burdens.

We understand the risks that corporates face in today's challenging business climate, and provide forensic accounting, data governance and compliance consulting services to help leading global organisations identify weaknesses, enhance compliance and integrity, and anticipate and mitigate future risk.

1740 Broadway
15th Floor
New York, NY 10019
United States
Tel: +1 646 808 1402

www.forensicrisk.com

Jenna Voss
jvoss@forensicrisk.com

Masako Asaka
masaka@forensicrisk.com

Umair Nadeem
unadeem@forensicrisk.com